I. AMENDMENT

A. In the Specification:

Please replace the paragraph on page 4, line 23 - page 5, line 5 to read as follows. A marked up copy of the paragraph showing insertions and deletions is attached to this Response in Appendix A.

A1

A preferred embodiment is a data encryption method performed with ring arithmetic operations wherein a modulus C is to be chosen of the form $2^w - L$, wherein C is a w-bit number and L is a low Hamming weight odd integer less than $2^{(w-1)/2}$. And in some of those embodiments, the residue mod C is calculated via several steps. P is split into 2 w-bit words H_1 and L_1. S_1 is calculated as equal to $L_1 + (H_1 2^{x1}) + (H_1 2^{x2}) + \ldots + (H_1 2^{xk}) + H_1$. S_1 is split into two w-bit words H_2 and L_2. S_2 is computed as being equal to $L_2 + (H_2 2^{x1}) + (H_2 2^{x2}) + \ldots + (H_2 2^{xk}) + H_2$. S_3 is computed as being equal to $S_2 + (2^{x1} + \ldots + 2^{xk} + 1)$. And the residue is determined by comparing S_3 to 2^w. If $S_3 < 2^w$, then the residue equals S_2. If $S_3 \geq 2^w$, then the residue equals $S_3 - 2^w$.

Please replace the paragraph on page 17, lines 2-7 to read as follows. A marked up copy of the paragraph showing insertions and deletions is attached to this Response in Appendix A.

A2

The shotgun multiplication method, as well as other methods, can be used more efficiently by choosing the bases ($m_1, \ldots m_{2l}$) in ways that make the modular calculations simpler. A w-bit number C is a "castout modulus" if it is of the form $2^w - L$, where L is a low Hamming weight odd integer less than $2^{(w-3)/2}$, i.e., $C = 2^w - 2^{x1} - 2^{x2} - \ldots - 2^{xk} - 1$, where $(w - 3)/2 > x_1 > x_2 > \ldots > x_k > 0$ and k is much less than w. The "castout order" of C is defined to be one less than the Hamming weight of L.

Please replace the abstract paragraph on page 37, lines 3-13 to read as follows. A marked up copy of the paragraph showing insertions and deletions is attached to this Response in Appendix A.

A3

A data encryption method performed with ring arithmetic operations wherein a modulus C is to be chosen of the form $2^w - L$, wherein C is a w-bit number and L is a low Hamming weight odd integer less than $2^{(w-1)/2}$. And in some of those embodiments, the residue mod C is calculated via several steps. P is split into 2 w-bit words H_1 and L_1. S_1 is calculated as equal to $L_1 + (H_1 2^{x1}) +$